CLAIMS

We claim:

1. A method for configuring an intrusion detection system in a network, comprising:

determining a location for a deployed intrusion detection sensor of said intrusion detection system wherein said sensor in enabled to monitor communication in a portion of said network;

deploying said intrusion detection sensor in said location in said network;

tuning said intrusion detection sensor to an appropriate level of awareness of content in said communication in said network;

prioritizing responses generated by said intrusion detection sensor to achieve an appropriate response to a detected intrusion in said network; and

configuring intrusion response mechanisms in said network to achieve an appropriate response by said mechanisms.

2. The method described in Claim 1 further comprising re-tuning said intrusion detection sensor in response to a prior intrusion detection.

3. The method described in Claim 1 wherein said network comprises communication protected by a firewall.

4. The method described in Claim 1 wherein said determining comprises determining a cost effective location in said network.

5. The method described in Claim 1 wherein said deploying comprises locating said sensor in a logical location in said network suitable to said monitoring said communication and to communicating out-of-band with said intrusion detection system.

6. The method described in Claim 1 wherein said prioritizing comprises enabling said intrusion detection sensor to scale a response to a determined level of threat posed by an intrusion.

7. The method described in Claim 1 wherein said network is a provisionable network.

8. The method described in Claim 7 wherein said provisionable network comprises a utility data center.

9. The method described in Claim 1 wherein said tuning comprises desensitizing said sensor to an intrusion representing a low probability of penetrating a firewall.

10. The method described in Claim 9 wherein said desensitizing comprises checking the attack signature of an intrusion against a set of firewall rules.

11. The method described in Claim 1 wherein said tuning comprises desensitizing said sensor to reduce false positive indications over an extended period.

12. A system for protecting security of a provisionable network, comprising:

a network server;

a pool of resources coupled with said server for employment by a client;

a resource management system for managing said resources; and

an intrusion detection system enabled to detect and respond to an intrusion in said network.

13. The system described in Claim 12 wherein said provisionable network comprises a utility data center.

14. The system described in Claim 12 wherein said intrusion detection system comprises an intrusion detection sensor.

15. The system described in Claim 12 wherein said intrusion detection sensor is tunable to determine a threat level posed by a detected intrusion.

16. The system described in Claim 15 wherein said intrusion detection system is tunable to generate a response appropriate to said threat level of said detected intrusion.

17. The system described in Claim 16 wherein said response comprises an alarm.

18. The system described in Claim 16 wherein said response comprises a lockout of a portion of said network.

19. A network intrusion detection system, comprising:

a network device comprising intrusion detection software, said device communicatively coupled with a provisionable network;

a trust hierarchy, comprising a portion of said network and enabled to communicate with said software and to cause evaluation of a detected intrusion;

a deployable, tunable, intrusion detection sensor; and

a network device enabled to generate a response to a detected intrusion.

20. The intrusion detection system described in Claim 19 wherein said network comprises a utility data center.

21. The intrusion detection system described in Claim 19 wherein said provisionable network comprises a resource pool.

22. The intrusion detection system described in Claim 19 wherein said provisionable network comprises a resource manager.

23. The intrusion detection system described in Claim 19 wherein said provisionable network comprises a network intrusion detection system.

24. The intrusion detection system described in Claim 19 wherein said providing a deployable intrusion detection probe is accomplished in said network intrusion detection system.

25. The intrusion detection system described in Claim 19 wherein said generating an alert based on said detection of said intrusion is accomplished in said network intrusion detection system.

26. The intrusion detection system described in Claim 19 wherein said trust hierarchy is configurable.

27. The intrusion detection system described in Claim 19 wherein said generating a response comprises initiating a lockout of a portion of said network.